

**Claims**

What is claimed is:

1. An online card-present transaction method comprising the steps of:  
accessing, within a host system, account information associated with an  
5 authenticated user; and  
communicating said account information over an authenticated  
communication channel from said host system to a merchant to facilitate a  
transaction between said merchant and said authenticated user.
2. The method of claim 1, said account information comprising said user's  
10 transaction account number.
3. The method of claim 2, said account information further comprising said  
user's name, address, transaction account expiration date, and delivery  
information.
4. The method of claim 1, wherein said communicating step occurs over the  
15 internet.
5. The method of claim 4, comprising the following steps for authenticating  
said user:  
receiving a user's browser that has been redirected from a merchant  
website to said host system website;  
20 issuing a challenge string to said user;  
prompting user to insert a smart card into a smart card reader and a enter  
personal identification number; and  
receiving a signed challenge string and valid digital certificate from said  
user.
- 25 6. The method of claim 5, further comprising the step of comparing said  
signed challenge string with said digital certificate to authenticate said user.
7. The method of claim 5, further comprising the step of comparing said  
signed challenge string and said digital certificate to information in a user  
database to authenticate said user.

8. The method of claim 1, further comprising the steps of:  
generating a secondary transaction number; and  
associating said secondary transaction number with said user's transaction  
account number, wherein said account information comprises said secondary  
transaction number in place of said transaction account number.

9. The method of claim 1, the step of communicating said account information  
over an authenticated communication channel further comprising the steps of:  
generating an encrypted host system signature;  
embedding said signature in a browsing window;  
directing said browsing window to said merchant, and  
causing said merchant to authenticate the identity of said host system by  
decrypting said signature.

10. The method of claim 8, further comprising the step of causing said  
merchant to validate account information communicated from said host system to  
said merchant.

11. The method of claim 1, the step of communicating said account information  
over an authenticated communication channel further comprising the steps of:  
communicating a host system token to said merchant over a first  
communication channel;

retrieving from said merchant, over a second communication channel, a  
request to verify that said host system issued said token; and  
confirming to said merchant that said host system issued said token.

12. The method of claim 10, further comprising the steps of:  
retrieving from said merchant, over a second communication channel, a  
request to verify that said host system issued said account information; and  
confirming to said merchant that said host system issued said account  
information.

13. The method of claim 1, comprising the additional steps of:  
obtaining merchant transaction field information necessary to facilitate  
transactions between said merchant and its customers;

storing said field information in a merchant database;

retrieving said field information from said merchant database to determine the type of said account information needed to complete transaction between said merchant and said user; and

5 retrieving account information from a user database corresponding to said field information.

14. A merchant interface method, comprising the steps of:

generating an encrypted host system signature;

embedding said signature in a browsing window;

10 directing said browsing window to said merchant, and

causing said merchant to authenticate the identity of said host system by decrypting said signature.

15 15. The method of claim 14, further comprising the step of causing said merchant to validate account information communicated from said host system to said merchant.

16. A merchant interface method, comprising the steps of:

communicating a host system token to a merchant over a first communication channel;

20 retrieving from said merchant, over a second communication channel, a request to verify that a host system issued said token; and

confirming to said merchant that said host system issued said token.

17. The method of claim 16, further comprising the steps of:

retrieving from said merchant, over a second communication channel, a request to verify that said host system issued said account information; and

25 confirming to said merchant that said host system issued said account information.

18. An online card present transaction method comprising the steps of:

receiving a user's browser that has been redirected from a merchant's website to a host system website;

30 sending said user a challenge string;

authenticating said user by receiving authentication information from said user, wherein said authentication information corresponds to a user's transaction account;

generating a secondary transaction number;

5 associating said secondary transaction number with said user's transaction account;

establishing an authenticated communication channel between said host system and said merchant; and

10 communicating said secondary transaction number over said authenticated communication channel to facilitate a transaction between said merchant and said user.

19. The method of claim 18, the step for establishing an authenticated communication channel comprising the following steps:

15 embedding an encrypted host system signature in said user's browser; and  
redirecting said user's browser to said merchant, causing said merchant to authenticate said host system by decrypting said host system signature.

20. The method of claim 18, the step for establishing an authenticated communication channel comprising the following steps:

20 communicating a token to said merchant over a first communication channel;

receiving a communication from said merchant over a second communication channel requesting said host system to confirm the issuance of said token; and

confirming to said merchant that said host system issued said token.

25 21. The method of claim 18, further comprising the steps of prompting said user to insert a smart card into a smart card reader and to enter a personal identification number.

22. The method of claim 18, wherein said authentication information comprises a signed challenge string and a digital certificate.

23. An online-card-present transaction method comprising the steps of:  
communicating with a user over a distributed network;  
recognizing the presence of an authentication device on a user's computer  
system;

5        redirecting user to a host system website, causing said host system to  
authenticate said user;

      establishing an authenticated communication channel with said host  
system; and

      receiving account information from said host system over said  
10    authenticated communication channel, wherein said account information facilitates  
completion of a transaction between said user and said merchant.

24. The method of claim 23, said establishing an authenticated communication  
channel step further comprising the steps of:

      receiving an encrypted host system signature; and

15        decrypting said encrypted host system signature to determine that said  
account information originated with said host system.

25. The method of claim 23, said establishing an authenticated communication  
channel step further comprising the steps of:

      receiving a host system token over a first communication channel, wherein  
20    said token identifies said host system; and

      communicating to said host system over a second communication channel  
to confirm that said token was issued by said host system.

26. A computerized merchant interface system comprising:

25        a means for communicating with a user and a merchant over a distributed  
network to facilitate an online transaction between said user and said merchant;

      a means for prompting said user to provide authenticating information;

      a means for receiving said authenticating information from said user;

      a means for accessing user account information associated with said user;

30        a means for establishing an authenticated communication channel between  
said host system and said merchant; and

a means for providing said account information to said merchant over said authenticated communication channel.

27. A computerized merchant interface method comprising the steps of:  
shopping at an online merchant's website over a distributed network using

5 a user's web browser;

selecting items to add to a virtual shopping cart;

selecting a smart card payment method;

causing said smart card to communicate with a smart card reader; and

entering a personal identification number, causing a host system to  
10 authenticate said user and to provide said merchant with account information to complete transaction with said merchant.

28. An online card-present transaction method, comprising the steps of:

receiving from a merchant over an authenticated communication channel, a  
user request to facilitate a transaction with said merchant;

15 communicating to a merchant a challenge string to facilitate a user authentication process;

retrieving from said merchant a signed challenge string and a digital  
certificate originating from said user, wherein said user is authenticated by  
comparing said signed challenge string and said digital certificate;

20 retrieving account information associated with said digital certificate; and

providing said account information to said merchant to facilitate said  
transaction.

25 29. The method of claim 28, wherein said authentication process comprises the further step of causing said user to insert a smart card into a smart card reader and input a personal identification number.

30. The method of claim 28, wherein the account information is a transaction account number.

31. The method of claim 28, comprising the further steps of:  
generating a secondary transaction number;

associating said secondary transaction number with said transaction account number; and

providing said merchant said secondary transaction account number in place of said transaction account number.

5 32. An online card-present system, comprising:

a user interface system configured to communicate with a user system to facilitate a transaction between said user and a merchant;

an authentication system electrically coupled to said web server system for accepting authenticating information from said user and invoking a user database  
10 to determine if said user is an authorized user; and

a smart card payment system electronically coupled to said web server for retrieving user account information and interfacing with said web server to provide said account information to said merchant to facilitate said transaction.

15 33. The system of claim 32, wherein said authenticating information comprises a signed challenge string and a digital certificate generated by communication between a smart card and a smart card reader.

20 34. The system of claim 32, further comprising a secondary transaction system configured to generate a secondary transaction number and associate said transaction number to said account information, wherein said secondary transaction number is provided to said merchant through said web server system.